(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－151091

(43)公開日　平成５年(1993)６月18日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/14	３２０　Ａ	9293－5B		
	1/00	３７０　Ｅ	7927－5B		
	12/14	３２０　Ｄ	9293－5B		

審査請求　未請求　請求項の数25(全 18 頁)

(21)出願番号　特願平3－312233

(22)出願日　平成３年(1991)11月27日

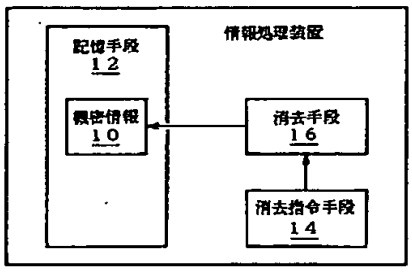
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　園部　正幸
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　竹内　進　（外１名）

(54)【発明の名称】　情報処理装置の機密情報管理方式

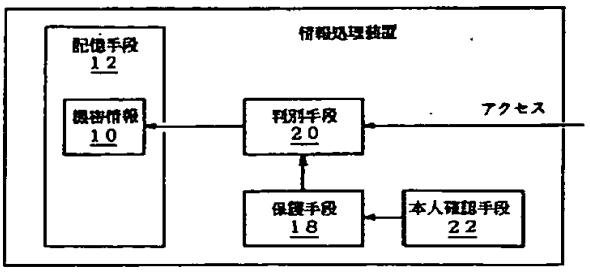
(57)【要約】
【目的】記憶装置に格納された機密情報が本人以外の第三者により利用されることを防止する情報処理装置の機密情報管理方式に関し、携帯時や長時間の離席に際して本人以外の者による機密情報の利用を簡単な操作で確実に防止することを目的とする。
【構成】記憶手段１２に格納した機密情報１０の消去を消去指令手段１４で指令した際に、消去手段１０が記憶手段１２の機密情報１０を消去する。例えば利用者のスイッチ操作時に自動的に機密情報１０を消去する。スイッチ操作等で機密情報１０のアクセス禁止を設定する保護手段１８を設け、判別手段２０でアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。アクセス禁止の設定解除は本人確認手段２２で行う。

本発明の原理説明図

(a)



(b)



1

【特許請求の範囲】

【請求項１】機密情報１０を格納した記憶手段１２と、前記機密情報１０の消去を指令する消去指令手段１４と、該消去指令手段１４の消去指令出力に基づいて前記記憶手段１２に格納された機密情報１０を消去する消去手段１６とを備えたことを特徴とする情報処理装置の機密情報管理方式。

【請求項２】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は操作スイッチを備え、利用者のスイッチ操作時に自動的に機密情報１０を消去することを特徴とする情報処理装置の機密情報管理方式。

【請求項３】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は装置の蓋を閉じることにより動作するスイッチを備え、装置の蓋を閉じた時に自動的に機密情報１０を消去することを特徴とする情報処理装置の機密情報管理方式。

【請求項４】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、外部からの電源供給の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項５】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、外部の電話線との接続断を電話線の電気状態から判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項６】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、外部の電話線の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項７】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、外部のモデムとの接続断をモデムとの間の電気状態で判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項８】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、外部のモデムの接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項９】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、パケット組立分解装置との接続断をパケット組立分解装置との間の電気状態で判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項１０】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、パケット組立分解装置の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

2

【請求項１１】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、ＩＣカードが抜かれたことを電気状態で判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項１２】請求項１記載の情報処理装置の機密情報管理方式に於いて、前記消去指令手段１４は、ＩＣカードが抜かれたことを接続部が外れたことで判別した時に消去指令を出力して自動的に機密情報１０を消去させることを特徴とする情報処理装置の機密情報管理方式。

【請求項１３】機密情報１０を格納した記憶手段１２と、前記機密情報１０のアクセス禁止を設定する保護手段１８と、機密情報１０のアクセスを受けて際に前記保護手段１８がアクセス禁止を設定していれば機密情報１０のアクセスを禁止し、アクセス禁止を解除していれば機密情報のアクセスを許容する判別手段２０と、利用者本人を確認して前記保護手段１８のアクセス禁止を設定解除する本人確認手段２２とを備えたことを特徴とする情報処理装置の機密情報管理方式。

【請求項１４】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は操作スイッチを備え、利用者のスイッチ操作時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項１５】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、装置の蓋を閉じることにより動作するスイッチを備え、装置の蓋を閉じた時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項１６】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、外部からの電源供給の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項１７】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、外部の電話線との接続断を電話線の電気状態から判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項１８】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、外部の電話線の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状

態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項１９】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１６は、外部のモデムとの接続断をモデムとの間の電気状態で判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項２０】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、外部のモデムの接続部が外れたことを判別しした時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項２１】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、パケット組立分解装置との接続断をパケット組立分解装置との間の電気状態で判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項２２】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、パケット組立分解装置の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項２３】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、ＩＣカードが抜かれたことを電気状態で判別しした時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項２４】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記保護手段１８は、ＩＣカードが抜かれたことを接続部が外れたことで判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【請求項２５】請求項１３記載の情報処理装置の機密情報管理方式に於いて、前記本人確認手段２２は、利用者が暗証コードを入力した時或いは装置の鍵を解錠した時に前記保護手段１８のアクセス禁止を設定解除して機密情報の読み書きを可能とする非保護状態に切替えることを特徴とする情報処理装置の機密情報管理方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、記憶装置に格納された機密情報が本人以外の第三者により利用されることを防止する情報処理装置の機密情報管理方式に関する。

【０００２】

【従来の技術】近年、携帯の容易な情報処理装置としてパーソナルコンピュータ、ワードプロセッサ、電子手帳等が広く普及している。こうした情報処理装置は、個人で利用されることが多く、更には企業機密にかかわるビジネスにも利用されており、情報処理装置に格納された機密情報の保護がプライバシーや企業秘密を守るために強く求められている。

【０００３】ここで機密情報の保護は、機密情報の読出し、書込み、または実行について考えられ、これらを総称して、アクセス（access）という。また、近年は会員制のパーソナルコンピュータの通信システムも広範に普及しており、システムの利用料金は持ち主に請求されるが、持ち主しか知らないＩＤ（利用者識別番号）やパスワード（暗証コード）を記憶装置に内蔵している機器においては、万一盗まれた場合、持ち主になりすまして使われてしまい、料金だけが持ち主に請求されるという問題が生じる。

【０００４】また、ファイルやデータベースを暗号化したときの暗号化鍵コードを知られると、ファイルやデータベースの中の機密情報にアクセスできてしまう。更に、さまざまな知人や会社等の機密情報が、記憶装置に内蔵されていたり、あるいは、盗まれた情報処理装置に持ち主の通信用のパスワードが含まれていて犯人に漏れた場合、機密情報の中にまた別の機密情報のパスワードが格納されている場合があり、機密情報がいったん漏洩すると、影響はどんどん拡大する。

【０００５】従って、情報処理装置を家庭やオフィスで使っているときには、機密情報を持ち主本人が自由に使えるほうがよいが、情報処理装置を外へ持出すときとか、席を外すときには、万一盗まれてもよいように、他人が機密情報に触れることを不可能な状態に簡単に切替えるということが要請される。従来の情報処理装置の機密保護にあっては、機密情報、情報サービス、動作或いは表示を暗証コードの入力で保護し、電源オンから暗証コード入力して不揮発性メモリに内蔵した正解の暗証コードと一致するまでは、機密情報、情報サービス、動作或いは表示をさせないといった技術が採用されている。

【０００６】

【発明が解決しようとする課題】しかしながら、暗証コードを入力するようにした従来の機密情報保護方式にあっては、機密情報を消去、或いは暗証コードまたは鍵を開けないと機密情報にアクセスできないように保護をかけることを管理ソフトウェアに命ずる操作が繁雑であり、使い難いために保護機能が有効に活用されない問題があった。

【０００７】また従来より記憶装置の全部の内容を消去するスイッチを設けた機器もあり、、操作は簡単であるが、これでは保護を必要としない多くの情報が一緒に消去されてしまう不都合があった。更に、暗証コードの入力により起動するタイマを設け、タイマの設定時間が経

過するまでは機密情報のアクセスを許容し、タイマの設定時間を超えると、再度暗証コードを入力しなければ機密情報の読み書き実行が不可能な保護状態に切替わる機密情報管理方式もある。

【０００８】しかし、タイマを用いた従来方式は、設定時間を短くすると、次に機密情報をアクセスする前に保護状態に切替わってしまうために頻繁に暗証コードの入力を必要とし、一方、タイマの設定時間を長くすると、席を外した時等に他人により機密情報が使われてしまう可能性が大きくなるという問題があった。本発明は、このような従来の問題点に鑑みてなされたもので、携帯時や長時間の離席に際して本人以外の者による機密情報の利用を簡単な操作で確実に防止できるようにした情報処理装置の機密情報管理方式を提供することを目的とする。

【０００９】

【課題を解決するための手段】図１は本発明の原理説明図である。まず本発明による情報処理装置の機密情報管理方式は、図１（ａ）に示すように、機密情報１０を格納した記憶手段１２と、機密情報１０の消去を指令する消去指令手段１４と、消去指令手段１４の消去指令出力に基づいて記憶手段１２に格納された機密情報１０を消去する消去手段１６とを備えたことを特徴とする。

【００１０】ここで消去指令手段１４は次の（１）～（１０）の形態をとる。

（１）操作スイッチを備え、利用者のスイッチ操作時に自動的に機密情報１０を消去する。

（２）装置の蓋を閉じることにより動作するスイッチを備え、装置の蓋を閉じた時に自動的に機密情報１０を消去する。

【００１１】（３）外部からの電源供給の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

（４）外部の電話線との接続断を電話線の電気状態から判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

（５）外部の電話線の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

【００１２】（６）外部のモデムとの接続断をモデムとの間の電気状態で判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

（７）外部のモデムの接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

（８）パケット組立分解装置との接続断をパケット組立分解装置との間の電気状態で判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

【００１３】（９）パケット組立分解装置の接続部が外れたことを判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

（１０）ＩＣカードが抜かれたことを電気状態で判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

（１１）ＩＣカードが抜かれたことを接続部が外れたことで判別した時に消去指令を出力して自動的に機密情報１０を消去させる。

【００１４】また本発明による情報処理装置の機密情報管理方式は図１（ｂ）に示すように、機密情報１０を格納した記憶手段１２と、機密情報１０のアクセス禁止を設定する保護手段１８と、機密情報１０のアクセスを受けて際に前記保護手段１８がアクセス禁止を設定していれば機密情報１０のアクセスを禁止し、アクセス禁止を解除していれば機密情報のアクセスを許容する判別手段２０と、利用者本人を確認して前記保護手段１８のアクセス禁止を設定解除する本人確認手段２２とをとを備えたことを特徴とする。

【００１５】ここで保護手段１８は次の（１）～（１１）の形態をとる。

（１）操作スイッチを備え、利用者のスイッチ操作時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

（２）装置の蓋を閉じることにより動作するスイッチを備え、装置の蓋を閉じた時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

【００１６】（３）外部からの電源供給の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

（４）外部の電話線との接続断を電話線の電気状態から判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

（５）外部の電話線の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

【００１７】（６）外部のモデムとの接続断をモデムとの間の電気状態で判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

（７）外部のモデムの接続部が外れたことを判別しした時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

【００１８】（８）パケット組立分解装置との接続断をパケット組立分解装置との間の電気状態で判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

（９）パケット組立分解装置の接続部が外れたことを判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

【００１９】（１０）ＩＣカードが抜かれたことを電気

状態で判別しした時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

（１１）ＩＣカードが抜かれたことを接続部が外れたことで判別した時にアクセス禁止を設定して機密情報１０の読み書きを不可能とする保護状態に切替える。

【００２０】更に図１（ｂ）の本人確認手段２２は、利用者が暗証コードを入力した時或いは装置の鍵を解錠した時に保護手段１８のアクセス禁止を設定解除して機密情報の読み書きを可能とする非保護状態に切替える。

【００２１】

【作用】このような構成を備えた本発明の情報処理装置の機密情報管理方式によれば、携帯や長時間離席に際してスイッチ操作、ＡＣ電源線の外し、外部通信回線と接続外し等を行うと、自動的に機密情報の消去や保護状態の設定が自動的行われ、操作がきわめて容易か特別な操作を必要とせず、機密情報の保護を確実に行うことができる。

【００２２】これにより、万が一、情報処理装置が盗難にあっても、盗難時の電源外しや通信回線の外しで機密情報が自動消去されたりアクセス不可能な保護状態に自動的に切替わり、その後の機密情報の利用を不可能にして悪用を未然に防止できる。

【００２３】

【実施例】図２は本発明の第１実施例の基本構成を示した実施例構成図である。図２において、２４は情報処理装置であり、例えばパーソナルコンピュータ，ワードプロセッサ，電子手帳等である。尚、以下の実施例にあっては情報処理装置２４としてパーソナルコンピュータを例にとって説明する。

【００２４】情報処理装置２４には記憶装置１２が設けられ、記憶装置１２の特定の記憶領域には機密情報１０が格納されている。また、情報処理装置２４には記憶装置１２の書込み，読出し、更には命令の実行を行う制御装置２６が設けられる。制御装置２６に対してはキーボードやマウス等により利用者からの操作入力が与えられ、この操作入力に基づくコマンドを実行する。

【００２５】本発明の機密情報管理方式にあっては、消去指令手段としてのスイッチ１４と消去部１６を新たに設けている。スイッチ１４は例えば情報処理装置２４のケースに設けられた操作スイッチであり、スイッチ１４をオン操作すると消去部１６に対し機密情報の消去指令が与えられる。消去部１６はスイッチ１４のオン操作による消去指令を受けると記憶装置１２に格納している機密情報１０を強制的に消去する処理を行う。

【００２６】図３は図２の情報処理装置２４に設けた消去部１６の処理動作を示したフローチャートである。図３において、まずステップＳ１で消去部１６はスイッチ１４のオン，オフを監視しており、スイッチ１４がオンされるとステップＳ２に進み、記憶装置１２の機密情報１０を強制的に消去する。

【００２７】具体的な使い方としては、例えば家庭や会社に情報処理装置を置いた通常の利用状態では情報処理装置２４をパワーオンスタートした動作状態にあれば自由に記憶装置１２の機密情報１０を機密情報１０以外の記憶情報と同様、制御装置２６からアクセスすることができる。一方、利用者が情報処理装置２４を例えば携帯して外出する場合や、あるいは電源を投入したまま長時間席を離れるような場合にはスイッチ１４を閉じる。スイッチ１４を閉じると、図３のフローチャートに示したように消去部１６が自動的に記憶装置１２内の機密情報１０を消去する。従って、その後第３者が情報処理装置２４を操作しても記憶装置１２内の機密１０は無くなっているので機密情報１０のアクセスは不可能となり、プライバシー情報やＩＤカード等の機密情報が第３者に知られてしまうことを確実に防止できる。

【００２８】更に、利用者が再び情報処理装置２４を使用する際に、もし機密情報１０が必要となれば再度自分で機密情報１０を記憶装置１２に入力するか外部システムの記憶装置と通信接続した情報入力により機密情報１０を作ることになる。図４は図２の実施例を具体化したラップトップ型のパーソナルコンピュータの説明図であり、図５に側面図を示す。

【００２９】図４において、ラップトップ型のパーソナルコンピュータとしての情報処理装置はキーボード２８を備えた計算機本体３０と、計算機本体３０に対し開閉自在なカバー部３２で構成され、カバー部３２の内側には液晶ディスプレイ３４が設けられている。計算機本体３０の右側面にはＩＣカード３６が挿入されている。また、図５の側面図から明らかなように、計算機本体３０の後部側にメインスイッチ３８が設けられ、更にＤＣコネクタ４０を設けている。このＤＣコネクタ４０に対しては、後の説明で明らかにするようにＡＣアダプタの出力端子が接続され、ＤＣコネクタ４０にＡＣアダプタの出力端子が接続されると自動的に計算機本体３０はそれまでのバッテリーモードから商用交流電源を使用して動作するＡＣモードに切り換わる。

【００３０】更に、計算機本体３０内には小型磁気ディスク装置としてハードディスク（ＨＤＤ）が格納されている。図４のパーソナルコンピュータにおいて、図２の実施例に示したスイッチ１４は計算機本体３０の前部右端に設けられており、スイッチ１４を消去位置に操作することで計算機本体３０内の記憶装置１２、例えばＲＡＭに格納されている機密情報１０を自動的に消去することができる。

【００３１】図６は図４，図５に示したラップトップ型パーソナルコンピュータにおける計算機本体３０の一実施例を示した実施例構成図である。図６において、計算機本体３０にはＣＰＵ４２が設けられ、ＣＰＵ４２からは内部バス４４が引き出される。ＣＰＵ４２に対しては制御プログラムを格納したＲＯＭ４６と一時的にデータ

を記憶保持するＲＡＭ４８が設けられる。本発明にあっては、ＲＡＭ４８の中に機密情報１０を格納している。

【００３２】また、ディスプレイコントローラ５０を介して液晶ディスプレイ３４が設けられ、ディスプレイコントローラ５０はビデオＲＡＭ５２に格納された画像データを表示する。このビデオＲＡＭ５２に格納された画像データについても、ＲＡＭ４８と同様、特定の情報を機密情報１０として扱うようにしてもよい。更にキーボードコントローラ５４を介してキーボード２８が接続される。

【００３３】内部バス４４の右側にはＩＣカードコントローラ５６とその入出力を行う入出力インタフェース５８及びＩＣカードアダプタ６０が設けられる。ＩＣカードアダプタ６０に対しては外部よりＩＣカード３６を着脱することができる。また、内部バス４４の右側にはディスクコントローラ６２との入出力インタフェース６４及び小型磁気ディスクを用いたハードディスク６６が設けられている。このハードディスク６６の出力情報についてもＲＡＭ４８と同様、特定の情報について機密情報１０として格納することができる。

【００３４】また、内部バス４４の右側にはプリントコントローラ６８との入出力インタフェース７０が設けられ、外部にプリンタ装置７２を接続することができる。更に、内部バス４４の右側には通信コントローラ７４との入出力インタフェース７６が設けられ、外部のモデム（変復調装置）７８を介して電話回線等の通信回線８０を接続することができる。

【００３５】これに加えて本発明の機密情報管理方式にあっては、内部バス４４に対し消去部１６が設けられ、消去部１６にはスイッチ１４が接続されている。消去部１６はスイッチ１４のオン操作による消去指令を受けた際に、例えば割込みをＣＰＵ４２に対し発行し、ＣＰＵ４２の制御のもとにＲＡＭ４８に格納されている機密情報１０の消去処理を行う。

【００３６】更に計算機本体３０には電源回路８２とバッテリー８４が設けられている。電源回路８２にはＤＣコネクタ４０が接続され、ＤＣコネクタ４０に対してはＡＣアダプタ８６の出力端子としてのプラグ８８が接続される。会社や家庭等において使用する際には、通常、ＡＣアダプタ８６のプラグ８８がＤＣコネクタ４０に接続され、ＡＣアダプタ８６は商用ＡＣ１００Ｖを受けて規定の直流電圧に整流平滑して電源回路８２に供給し、電源回路８２は各回路部に規定の電源電圧を供給する。

【００３７】一方、外出先等で使用する際には商用電源を取ることができないため、ＤＣコネクタ４０からＡＣアダプタ８６のプラグ８８は外されており、この状態ではバッテリー８４から電源回路８２に電源供給が行われる。尚、ＡＣアダプタ８６の使用時には、電源回路８２を介してバッテリー８４の充電が同時に行われる。図７は図２に示したスイッチ１４のラップトップ型パーソナルコンピュータにおける他の実施例を示した説明図である。

【００３８】図７の実施例にあっては、計算機本体３０のキーボード２８の設置面の左上隅にスイッチ１４を設け、このスイッチ１４に相対するカバー部３２の内側に突起９０を設けている。スイッチ１４は図示のカバー部３２を開放した状態では、図示のように突出して例えばスイッチオフ状態にあり、図２に示した消去部１６に対する消去指令の出力を禁止している。

【００３９】一方、外出時や席を離れる際にカバー部３２を閉じると、カバー部３２の内側に設けた突起９０が計算機本体９０側のスイッチ１４を押圧してスイッチ１４がオンし、これにより記憶装置の機密情報１０の消去が自動的に行われる。この図７の実施例にあっては、機密情報を消去するための特別な操作は必要とせず、カバー部３２を閉じることで自動的に機密情報の消去ができる。

【００４０】図８は本発明の消去指令手段の他の実施例を示した実施例構成図であり、この実施例にあっては、ＡＣアダプタ８６のプラグ８８をＤＣコネクタ４０から抜いたことを判別して機密情報を自動的に消去するようにしたことを特徴とする。図８は装置本体側のＤＣコネクタ４０にＡＣアダプタのプラグ８８を差し込んだ状態を示す。

【００４１】プラグ８８は中央先端に突出した電極部９２と絶縁部９４を介して背後に設けた電極部９６を有し、この実施例にあっては、電極部９２がマイナス側、電極部９６がプラス側となっている。ＤＣコネクタ４０は中央先端の電極部９２に接触する接点部材９８と電極部９６に接触する外側の接点部材１００を備える。接点部材９８は内部のマイナスライン１０２に接続され、また接点部材１００は内部のプラスライン１０４に接続される。プラスライン１０４とマイナスライン１０２の間にバッテリー８４が接続される。このうちプラスライン１０４からは抵抗１０６とダイオード１０８の充電回路を介してバッテリー８４のプラス側が接続される。

【００４２】バッテリーのプラス側はＤＣコネクタ４０のスイッチ部材１１０に接続される。スイッチ部材１１０は図示のようにプラグ８８を差し込んだときの接点部材１００の外側への変形でプラスライン１０４との接続が切り話されている。更に、ＤＣコネクタ４０にはスイッチ部材１１２が設けられる。スイッチ部材１１２はスイッチ部材１１０とは逆にプラグ８８を差し込むと図示のようにプラスライン１０４に接続される。

【００４３】バッテリー８４の出力側には図２の消去部１６に対し消去指令信号を出力するためのフリップフロップ１１４が接続され、フリップフロップ１１４の入力にはＤＣコネクタ４０のスイッチ部材１１２が接続される。１１６は入力用の抵抗である。図８のプラグ８８を差し込んだ状態にあっては、ＡＣアダプタで整流された

直流電圧がＤＣコネクタ４０を介してプラスライン１０４及びマイナスライン１０２により直接装置の電源回路に供給されている。このときスイッチ部材１１０は接点部材１１０から離れており、従ってバッテリー８４はプラスライン１０４より抵抗１０６及びダイオード１０８を介して充電電流を受ける。

【００４４】一方、スイッチ部材１１２が接点部材１００に接触していることからフリップフロップ１１４にＨレベル入力が行われ、フリップフロップ１１４はセット状態となることで消去部１６に対し消去指令信号の出力を停止している。図９は図８のプラグ８８をＤＣコネクタ４０から抜いた状態を示す。プラグ８８をＤＣコネクタ４０から抜くと、接点部材９８及び１００は変形状態から元の水平な状態に戻る。このため、接点部材１００に対するスイッチ部材１１２の接触が断たれ、同時にスイッチ部材１１０が接点部材１００に接触する。

【００４５】これによって、バッテリー８４からのプラス電圧がスイッチ部材１１０，接点部材１００を介してプラスライン１０４に供給され、バッテリー８４による電源供給状態に切り換わる。同時にスイッチ接点１１２が離れることでフリップフロップ１１４に対する入力がＬレベルに立ち下がり、フリップフロップ１１４がリセットされることで消去部１６に対し消去指令信号を出力し、プラグ８８を抜くと自動的に機密情報の消去が行われる。

【００４６】尚、図８，図９の実施例ではプラグ８８を書き込んだときにフリップフロップ１１４をセットしプラグ８８を抜いたときにフリップフロップ１１４をリセットしているが、逆にプラグ８８の差し込みでフリップフロップ１１４をリセットしプラグ８８を抜くことでフリップフロップ１１４をセットするようにしてもよい。

【００４７】このような図８，図９に示す外部から電源供給の接続部が外れたことを判別して機密情報を自動的に消去できるようにすることで、家庭や会社で使用している場合には通常、ＡＣアダプタを接続して外部から電源供給しているが、外出時には当然にＡＣアダプタを外すことから、外部からの電源供給の接続が外れることで自動的に機密情報の消去が行われる。また、席を長時間離れるような場合にもＡＣアダプタを外しておけば、同様に機密情報が消去できる。

【００４８】図１０は本発明の消去指令手段の他の実施例をラップトップ型パーソナルコンピュータの計算機本体３０について示した実施例構成図である。この図１０の実施例にあっては、消去部１６に対する消去指令を監視部１１６より出力するようにしたことを特徴とする。監視部１１６はこの実施例にあっては、ＩＣカードアダプタ６０に対するＩＣカード３６の着脱状態、通信回線８０を接続したモデム７８の状態、更に電源回路８２に対する外部からの電源供給状態を監視している。

【００４９】監視部１１６の具体的な実施例としては、

次の　～　がある。

外部からの電源回路８２に対する電源供給の接続部が外れたことを判別して消去部１６に対し消去指令信号を出力する。

モデム７８に通信回線８０として電話回線を接続している場合、電話回線の接続断を電話回線の電気状態で判別して消去部１６に消去指令信号を出力する。

【００５０】　　と同様、通信回線８０として電話回線を接続している場合、電話回線の接続部、例えばモジュラージャック等が外れたことを判別して消去部１６に消去指令信号を出力する。

モデム７８との接続断をモデム７８との電気状態、例えばキャリア有無で判別し、キャリア無しを判別したときに消去部１６に対し消去指令信号を出力する。

【００５１】　モデム７８と接続しているケーブル接続部が外れたことを判別して消去部１６に消去指令信号を出力する。

通信回線８０によりパケット通信を行う場合に、モデム７８に内蔵されたパケット組立分解装置（ＰＡＤパケットアッセンブリ・リアッセンブリ装置）との接続断をパケット組立分解装置との間の電気状態で判別して消去部１６に消去指令信号を出力する。

【００５２】　モデム７８に設けたパケット組立分解装置のケーブル接続が外れたことを判別して消去部１６に消去指令信号を出力する。

ＩＣカードアダプタ６０からＩＣカード３６が抜かれたことを電気状態で判別して消去部１６に消去指令信号を出力する。

ＩＣカードアダプタ６０からＩＣカード３６が抜かれたことをＩＣカード３６とＩＣカードアダプタ６０の接続部が外れたことで判別して消去部１６に消去指令信号を出力する。

【００５３】図１１は本発明の第２実施例の基本構成を示した実施例構成図である。図１１において、情報処理装置２４には機密情報１０を格納した記憶装置１２が設けられ、制御装置２６により外部からの指令に基づいて機密情報１０を含む記憶情報のアクセスが行われる。機密情報１０を保護するため、この実施例にあっては保護部１８を構成するセット回路部１２０と保護フリップフロップ１２４、制御装置２６の１つの機能として設けられる判別部２０、更に保護フリップフロップ１２４のリセットを行う本人確認部２２が設けられる。セット回路部１２０はスイッチ１４のオン，オフに基づいて保護フリップフロップ１２４に対するセット動作を行う。

【００５４】情報処理装置２４の電源を投入してパワーオンスタートさせた状態にあっては保護フリップフロップ１２４はリセット状態にあり、判別部２０に対し非保護を指令している。このため、制御装置２６は記憶装置１２の機密情報１０をアクセスすることができる。一方、スイッチ１４をオンするとセット回路部１２０が保

護フリップフロップ１２４をセットして保護状態に設定する。この保護状態にあっては、制御装置２６の判別部２０がアクセスを受けた際に保護フリップフロップ１２４の保護状態を判別し、もし機密情報１０に対するアクセスであれば、このアクセスを禁止する。

【００５５】従って、外出の際や長時間席を離れる際にスイッチ１４を操作しておけば自動的に機密情報１０に対する制御装置２６からの読み書きを不可能とする保護状態に切り換えることができる。一度セット状態となった保護フリップフロップ１２４は本人確認部２２における本人確認に基づいてリセットされ、非保護状態とすることができる。本人確認部２２における本人確認の手法としては、電磁気的な紙の操作、ＩＤカードやＩＣカードの差し込み等の公知の方法を用いることができる。

【００５６】尚、上記の実施例では、電源投入をしたパワーオンスタート時に保護フリップフロップ１２４を最初リセット状態としているが、保護を確実にするためには、パワーオンスタート時に保護フリップフロップ１２４をセット状態とし、本人確認部２２に対する確認処理を行って初めて保護フリップフロップ１２４をリセットして非保護とできるようにすることができる。このようにすれば、本人確認部２２による本人確認を一度行えばスイッチ１４をオンするまでは何回では機密情報１０をアクセスすることができる。

【００５７】図１２は図１１の制御装置２６に設けた判別部２０による機密保護処理を示したフローチャートである。図１２において、まず装置をパワーオンスタートするとステップＳ１で機密情報のアクセスの有無を監視しており、機密情報のアクセスでなければステップＳ３に進んでアクセスを許可する。一方、機密情報のアクセスであった場合にはステップＳ２で保護フリップフロップ１２４がセット状態か否かチェックする。セット状態になければ非保護であることからステップＳ３に進んでアクセスを許可する。セット状態にあれば保護であることからステップＳ４に進み、機密情報のアクセスを禁止する。

【００５８】図１３は図１１の実施例をラップトップ型パーソナルコンピュータに適用した場合の計算機本体３０の実施例構成図である。この図１３の実施例にあっては、ＣＰＵ４２からの内部バス４４に対し保護フリップフロップ１２４の出力を供給し、保護フリップフロップ１２４はスイッチ１４を備えたセット回路部１２０によりセットできるようにしている。また、保護フリップフロップ１２４のリセットはＩＣカード３６の挿入等によるＣＰＵ４２による本人確認の処理結果を内部バス４４より受けてリセットする。

【００５９】それ以外の計算機本体３０の構成は図６の実施例と同じである。また図１３の実施例におけるスイッチ１４としては、図４の計算機本体３０の前部に設けたスイッチ１４、図７の計算機本体３０のキーボード面の隅に設けたスイッチ１４とカバー部３２の突起９０により蓋を閉じることでオンするスイッチ、更に図８，図９に示したＡＣアダプタのプラグ８８のＤＣコネクタ４０に対する着脱を検出する実施例のいずれかをそのまま適用することができる。

【００６０】尚、図８，図９の実施例にあっては、フリップフロップ１１４を図１３の保護フリップフロップ１２４としてもよい。更に図１３の実施例についても、図１０の実施例と同様、スイッチ１４の代わりに監視部１１６を設け、図１０について前述した　～　のいずれかの状態を判別したときにセット回路部１２０よりセット信号を保護フリップフロップ１２４に出力して保護フリップフロップを保護状態に設定し、機密情報１０のアクセスを禁止させるようにしてもよい。

【００６１】更に上記の実施例は機密情報の自動消去とアクセスを禁止する保護モードへの切替えを例にとるものであったが、情報処理装置に消去機能と保護機能の２つを設け、暗証コード等の入力で機密情報の自動消去モードと保護モードとを切替えできるようにしてもよい。更に、上記の実施例はラップトップ型パーソナルコンピュータを例にとるものであったが、本発明はこれに限定されず、個人的に使用されるワードプロセッサや電子手帳等の適宜の情報処理装置にそのまま適用することができる。

【００６２】

【発明の効果】以上説明してきたように本発明によれば、情報処理装置を携帯する場合や長時間席を離れる場合に機密情報を消去するかあるいは機密情報のアクセスを禁止する保護状態を簡単な操作あるいは特別な操作を必要とすることなく実現でき、第三者に機密情報が見られたり盗難時に機密情報が知られて悪用されてしまう等の問題を未然に防止でき、情報処理装置の小形化に伴う機密保護の強い要求に適切に対応することができる。

【図面の簡単な説明】

【図１】本発明の原理説明図

【図２】本発明の基本的な第１実施例を示した実施例構成図

【図３】図２の実施例による機密情報の消去処理を示したフローチャート

【図４】図２の実施例を適用したパーソナルコンピュータの説明図

【図５】図４の側面図

【図６】図４の計算機本体の実施例構成図

【図７】蓋の閉鎖でスイッチを作動して機密情報を消去させるパーソナルコンピュータの説明図

【図８】ＡＣアダプタのプラグ抜きを検出して機密情報を消去させる回路のプラグ装着状態の実施例構成図

【図９】図８についてプラグを抜いた状態を示した実施例構成図

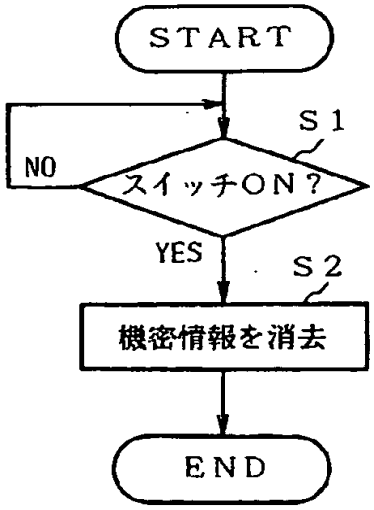
【図１０】監視部により機密情報の消去条件を判別する

15　　16

ようにした計算機本体の他の実施例構成図
【図１１】本発明の基本的な第２実施例を示した実施例構成図
【図１２】図１０の実施例による機密情報の保護処理を示したフローチャート
【図１３】図１１の実施例を適用したマイクロコンピュータ計算機本体の実施例構成図
【符号の説明】
１０：機密情報
１２：記憶手段
１４：消去指令手段（スイッチ）
１６：消去手段（消去部）
１８：保護手段（保護部）
２０：判別手段（判別部）
２２：本人確認手段（本人確認部）
２４：情報処理装置
２６：制御装置
２８：キーボード
３０：計算機本体
３２：カバー部
３４：液晶ディスプレイ
３６：ＩＣカード
３８：メインスイッチ
４０：ＤＣコネクタ
４２：ＣＰＵ
４４：内部バス
４６：ＲＯＭ
４８：ＲＡＭ
５０：ディスプレイコントローラ
５２：ビデオＲＡＭ
５４：キーボードコントローラ
５６：ＩＣカードコントローラ
５８，６４，７０，７６：入出力インタフェース
６０：ＩＣカードアダプタ
６２：ディスクコントローラ
６６：ハードディスク
６８：プリンタコントローラ
７２：プリンタ装置
７４：通信コントローラ
７８：モデム
８０：通信回線
８２：電源回路
８４：バッテリー
８６：ＡＣアダプタ
８８：プラグ
９０：突起
９２，９６：電極
９４：絶縁部
９８，１００：接触部材
１０２：マイナスライン
１０４：プラスライン
１０６，１１６：抵抗
１０８：ダイオード
１１０，１１２：スイッチ部材
１１４：フリップフロップ（ＦＦ）
１１６：監視部
１２０：セット回路部
１２４：保護フリップフロップ

【図３】

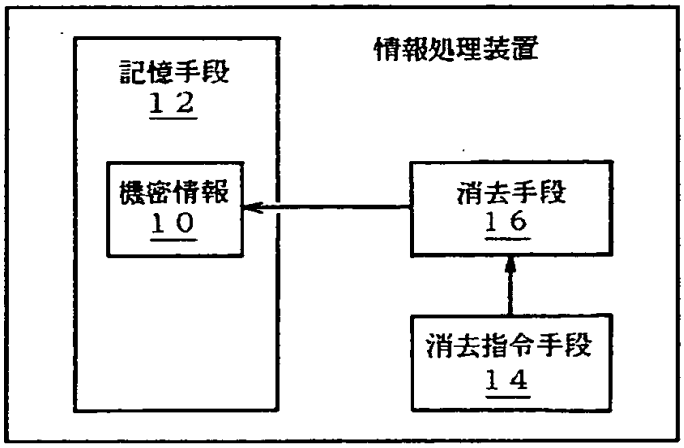
図２の実施例による機密情報の消去処理を示したフローチャート



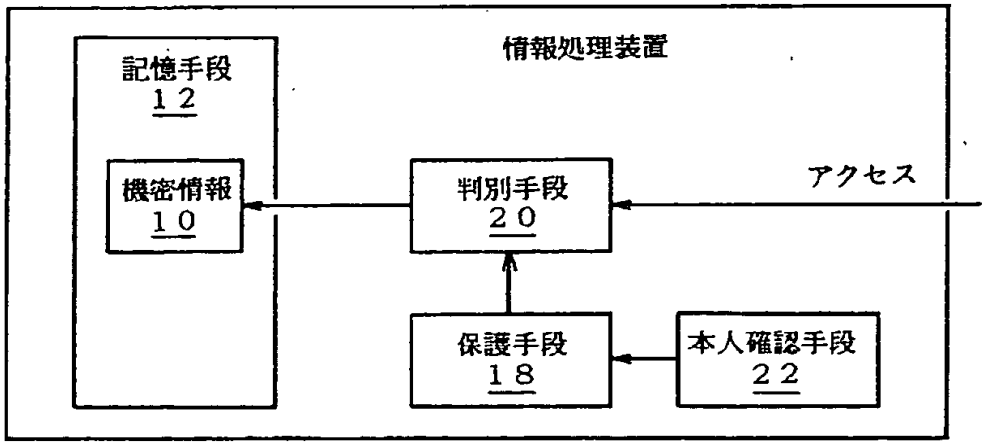
【図１】

本発明の原理説明図

（ａ）

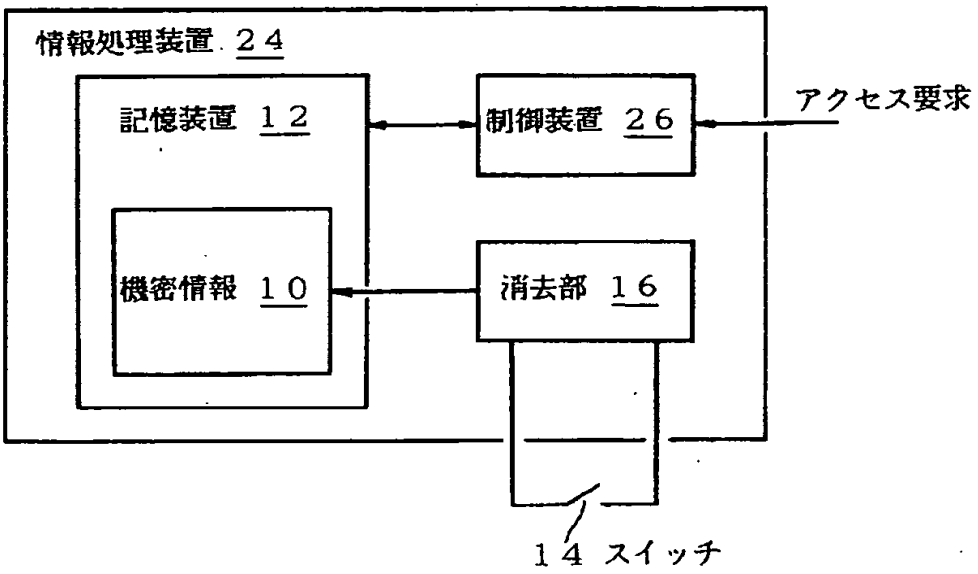


（ｂ）



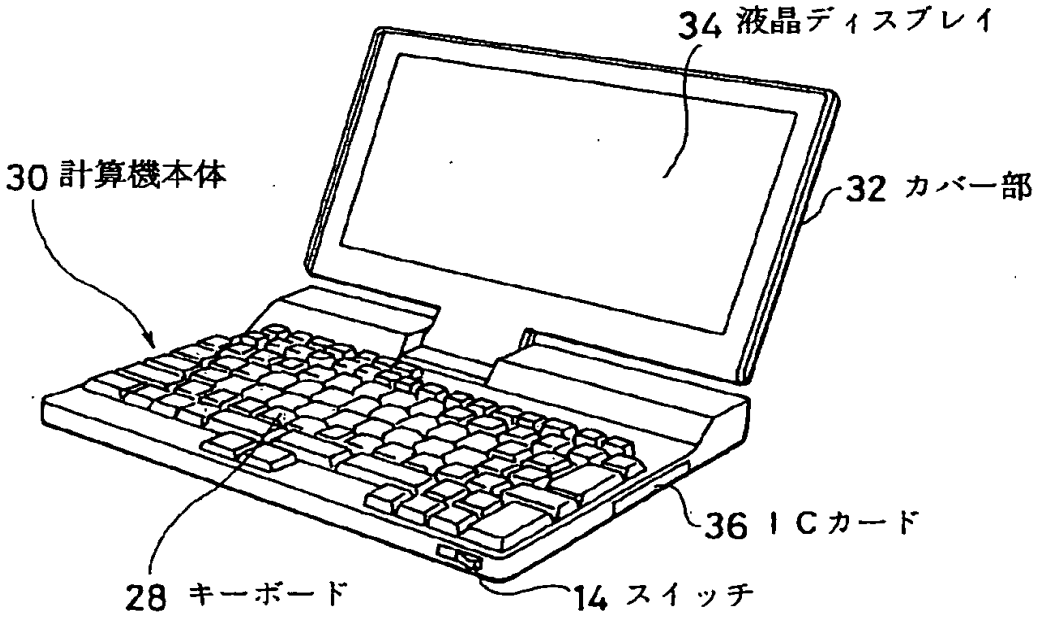
【図２】

本発明の基本的な第１実施例を示した実施例構成図



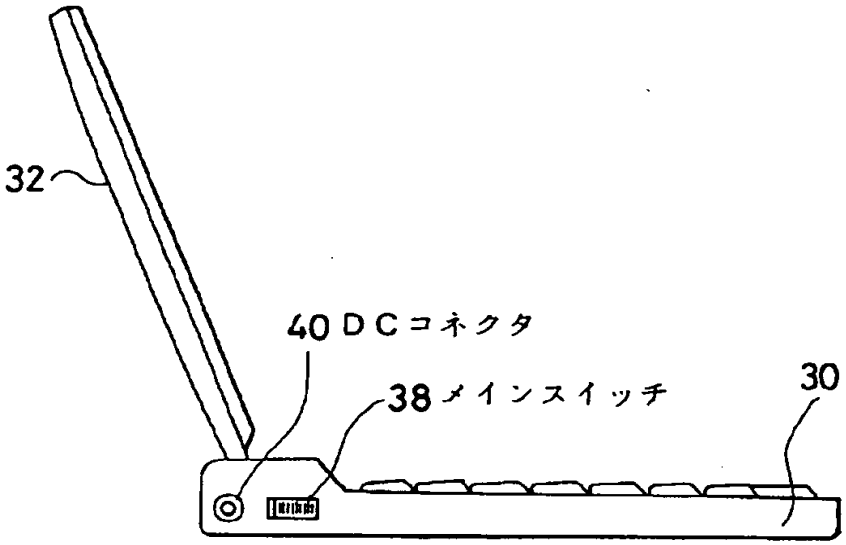
【図４】

図２の実施例を適用したパーソナルコンピュータの説明図



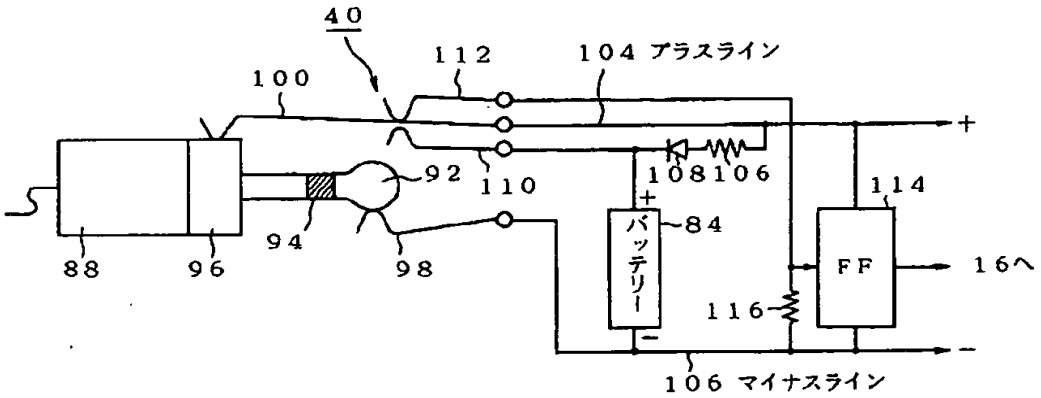
【図５】

図４の側面図



【図８】

ＡＣアダプタのプラグ抜きを検出して機密情報を消去させる回路のプラグ装着状態の実施例構成図



【図６】

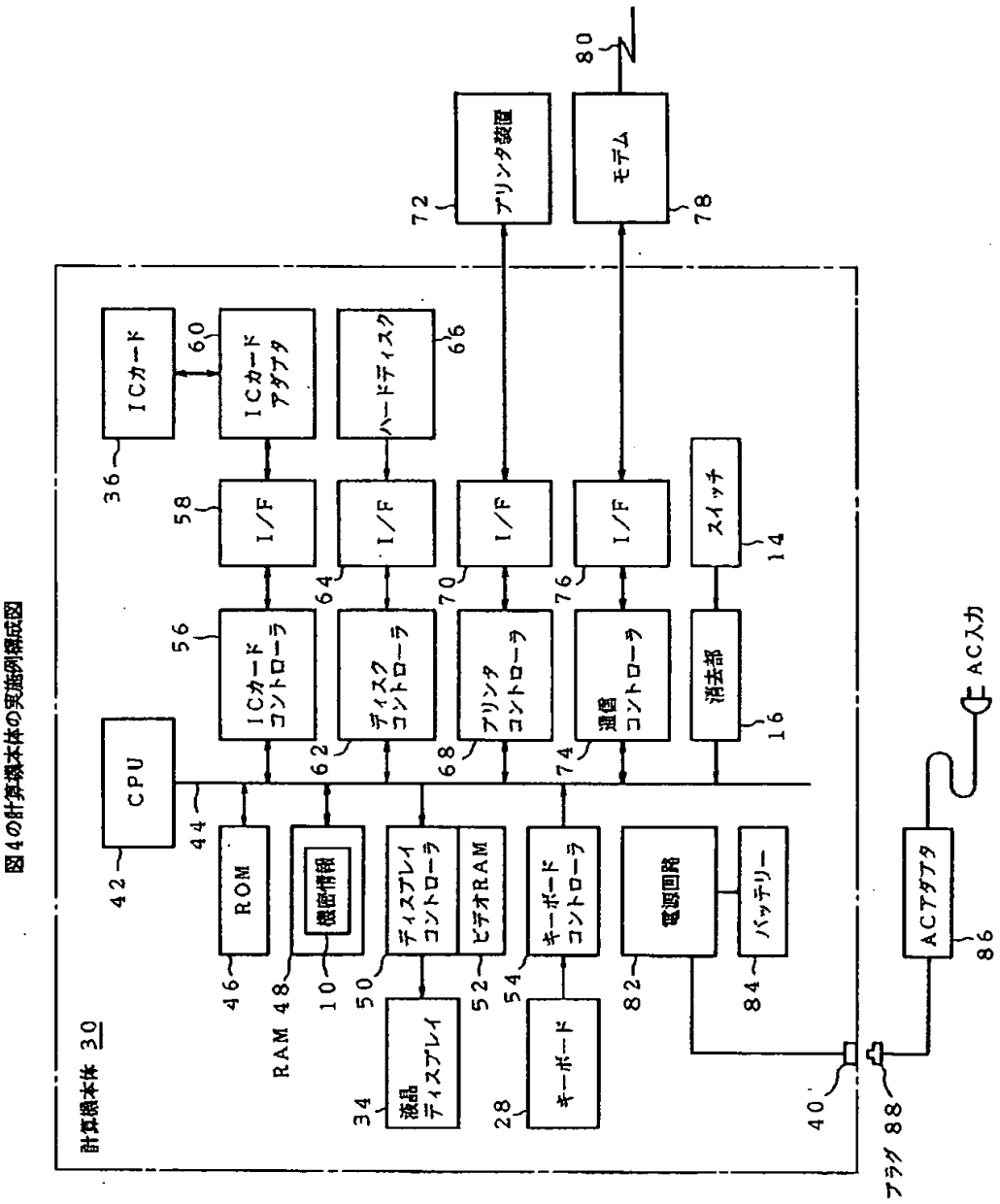
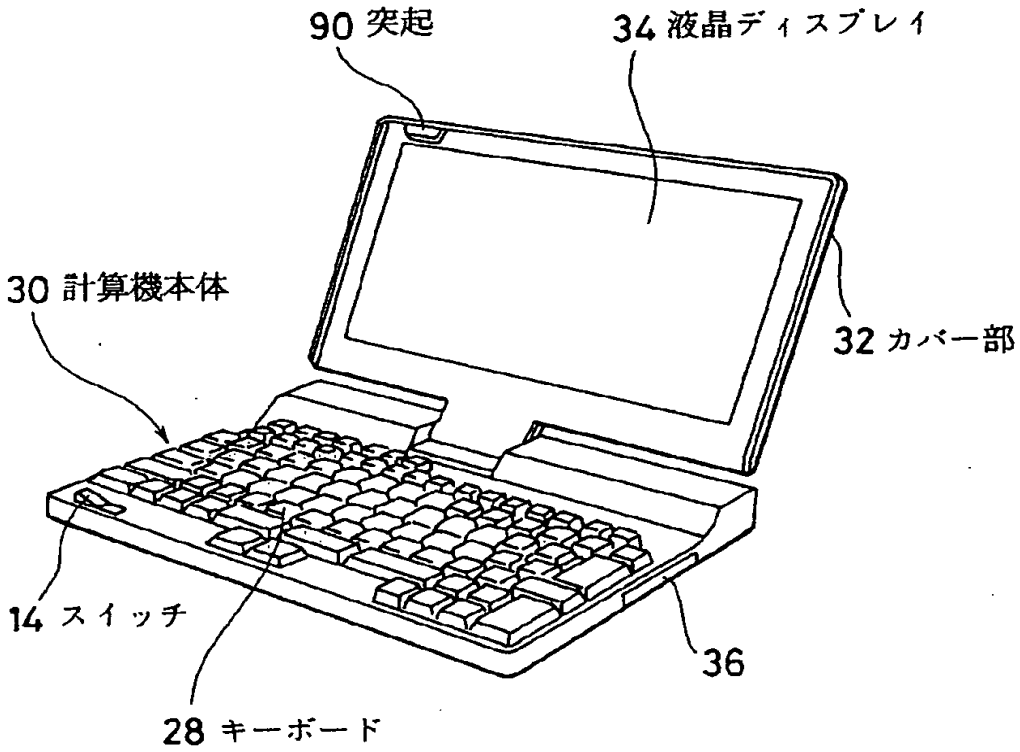


図４の計算機本体の実施例構成図

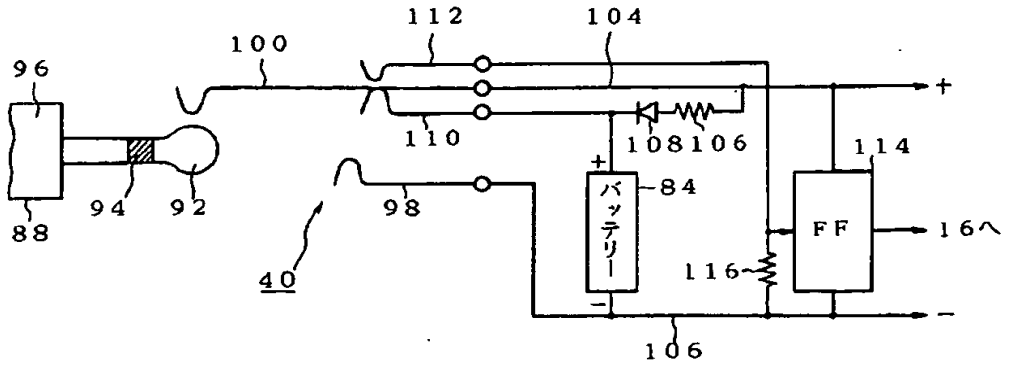
【図7】

蓋の閉鎖でスイッチを作動して機密情報を消去させる
パーソナルコンピュータの説明図



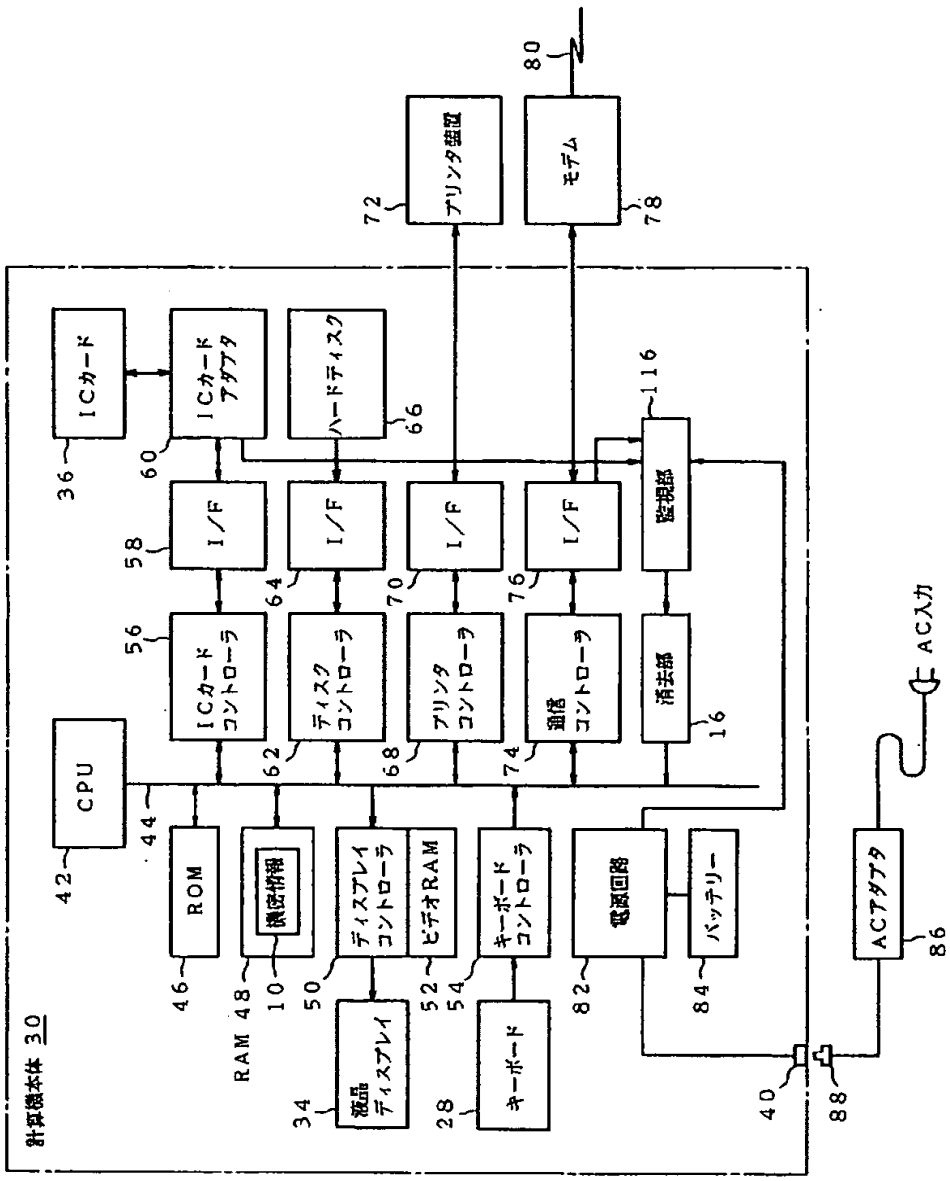
【図9】

図8についてプラグを抜いた状態を示した実施例構成図



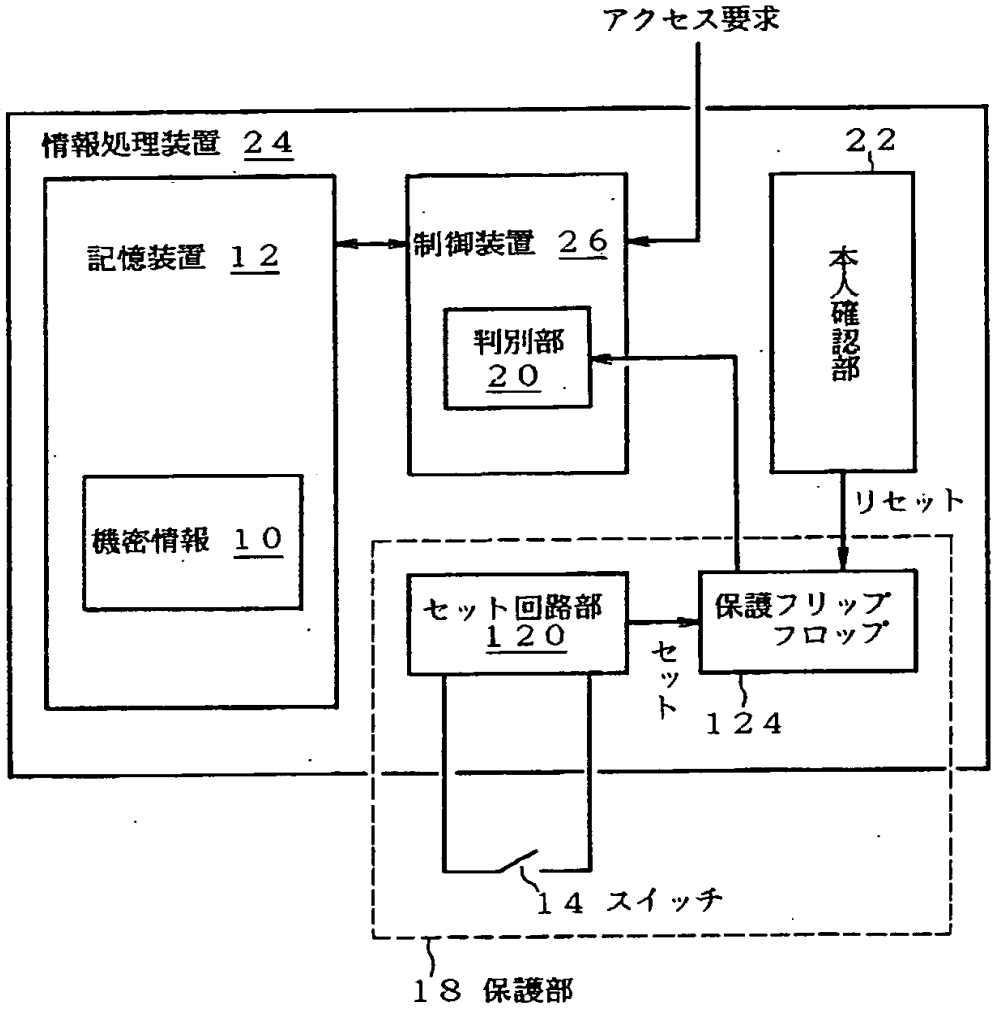
【図１０】

監視部により機密情報の消去条件を判別するようにした計算機本体の他の実施例構成図



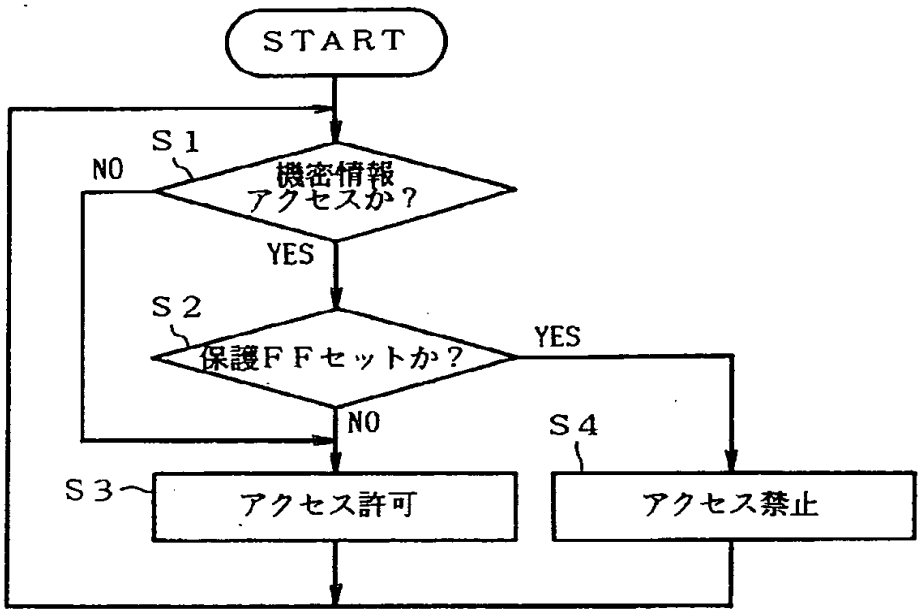
【図１１】

本発明の基本的な第２実施例を示した実施例構成図



【図１２】

図１０の実施例による機密情報の保護処理を示したフローチャート



【図１３】

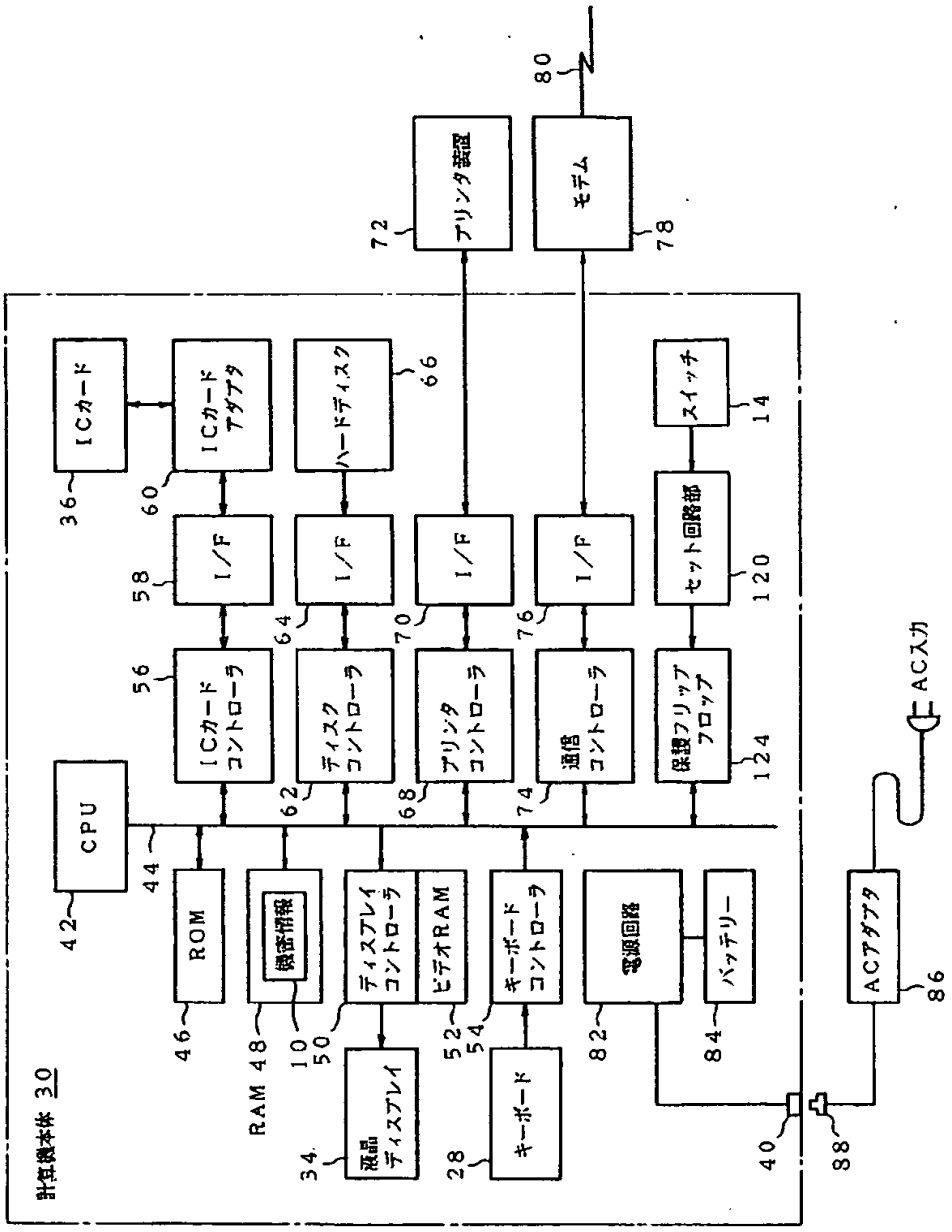


図１１の実施例を適用したマイクロコンピュータ計算機本体の実施例構成図